

Second Supplemental Hochman Report

**Redacted Version of
Document Sought to
be Sealed**

Table of Contents

I. Introduction3

II. Executive Summary of Opinions.....3

III. Statement of Limitations Regarding this Report4

IV. Engagement.....4

V. Preparation5

VI. Opinions.....5

 A. Google’s ██████████ Private Browsing Detection Bit 5

 1. ██████████ Is Unique..... 5

 2. Google Used ██████████ for Multiple Years..... 6

 3. Google’s Refusal to Investigate Additional Bits 7

 4. The ██████████ Bit Supports My Prior Opinions..... 9

 B. ██████████ Additional Google Logs with Incognito Detection Bits 13

 1. Google Discloses the Logs, but Does Not Conduct a Full Investigation..... 13

 2. The ██████████ New Logs Support My Prior Opinions..... 16

I. INTRODUCTION

1. This supplemental report addresses information that Google provided after I served my prior expert report, on June 7, 2022. I understand from Counsel that this new information came to light because or, or at least during, the sanctions proceedings in this case, and that Google did not provide any of this information during the discovery period in this case.

2. The new information I address in this report includes:

- The [REDACTED] private browsing detection bit, which Google first disclosed to Plaintiffs on December 20, 2022 (Dec. 20, 2022 Ltr. from Google’s Counsel).
- The [REDACTED] additional logs that contain Incognito detection bits, including the “[REDACTED]” that contains [REDACTED] (Martin Sramek June 14, 2022 and August 18, 2022 Declarations; Vasily Panferov November 30, 2022 Declaration; Google’s November 30 Response to the Court’s Order to Show Cause). Google did not disclose any of these logs until June 14, 2022—after I served my second and final expert report on June 7, 2022, and after the Court issued its first sanctions order on May 20, 2022.

3. I am not offering any new opinions in this report. The purpose of this report is to explain how the new information Google provided further substantiates several opinions I already offered in my April 15, 2022 opening report and my June 7, 2022 rebuttal and supplemental report. Had I known about this information when I prepared those reports, I would have relied on it in further support of the opinions offered.

II. EXECUTIVE SUMMARY OF OPINIONS

4. Pursuant to the Court’s Standing Order, this section includes an executive summary of each opinion to be proffered in this report.

5. Opinion 1: The information that Google has provided about [REDACTED] provides additional support for my already asserted opinions, including my opinions about Google’s interception, storage, and use of private browsing data, Google’s ability to identify private browsing traffic and class members, and Google’s ability to delete the private browsing data it has already collected. This new information also undermines opinions asserted by Google’s experts and contradicts Google’s prior representations.

6. Opinion 2: The information that Google has provided about [REDACTED] additional logs with Incognito detection bits provides additional support for my already asserted opinions, including my opinions about Google’s interception, storage, and use of private browsing data, Google’s ability to identify private browsing traffic and class members, Google’s ability to delete the private browsing data it has already collected, and Google’s ability to destroy algorithms developed through that data. This new information also undermines opinions asserted by Google’s experts and contradicts Google’s prior representations.

III. STATEMENT OF LIMITATIONS REGARDING THIS REPORT

7. I prepared this supplemental report for purposes of this case only. It may not be used for any other purpose. This report contains and refers to information designated as “CONFIDENTIAL” and “HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY” under a Stipulated Protective Order.

IV. ENGAGEMENT

8. Counsel for the Plaintiffs in this action (“Counsel”) retained me to develop and render opinions concerning the technology and practices at issue in this litigation with respect to several products developed and distributed by defendant Google, LLC (“Google”). The Google Products include Chrome Incognito and Google tracking code (e.g., Google Analytics and conversion tracking code) and Google advertising code (e.g., Google Ad Manager and Google AdSense

advertising code). I submitted my opening expert report on April 15, 2022. My opening report contained a section outlining my expertise, and my CV was included as Exhibit A to that report. On June 7, 2022, I submitted my Rebuttal to Report of Georgia Zervas and Supplemental Report of Jonathan Hochman.

9. An updated copy of my CV is attached to this supplemental report as **Exhibit A**.

10. As before, I am being compensated at the rate of \$800/hour and my associate, Julie Ann Burns, is being compensated at an hourly rate of less than \$800/hour. Our compensation does not depend upon the outcome of the case. In the event of any recovery in this case, I understand that Ms. Burns and I will be excluded from any disbursement of funds.

V. PREPARATION

11. As discussed in both my opening report and my rebuttal and supplemental report, I spent hundreds of hours reviewing materials produced in this case, including documents Google produced as well as deposition transcripts and written discovery responses. I also reviewed extensive data from Google's logs produced through the Special Master process.

12. In preparing this supplemental report, I worked with the consultants identified in my opening and rebuttal reports, including to analyze the new information that Google provided and which is addressed in this report.

VI. OPINIONS

A. Google's [REDACTED] Private Browsing Detection Bit

1. [REDACTED] Is Unique

13. This newly disclosed bit is different from the three previously disclosed Incognito detection bits (maybe_chrome_incognito, is_chrome_incognito, and is_chrome_non_incognito) in at least two ways.

14. First, the [REDACTED] previously disclosed bits detect Chrome Incognito traffic by way of the X-Client-Data Header, which is unique to the Chrome browser. This new bit detects private browsing traffic for several different browsers, including Chrome, Safari, Firefox, Edge, and Edge Legacy. This new bit is therefore relevant to both Class 1 and Class 2.

15. Second, the [REDACTED] bit does not rely on the X-Client-Data Header and instead relies on an entirely different signal. As explained by Google engineer Borbála Katalin Benkő in her December 21, 2022 declaration, “The [REDACTED] field is [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] (Benkő Dec. 21, 2022 Decl. ¶ 5). Ms. Benkő further explained that [REDACTED]
and that Google [REDACTED]
[REDACTED] (*Id.*).

2. Google Used [REDACTED] for Multiple Years

16. Google used the [REDACTED] bit for a significant portion of the class period. Google began using it on October 13, 2016, which is shortly after the June 1, 2016 beginning of the class period (*Id.* ¶ 3). Google changed what it refers to as the “[REDACTED] API in 2019, which presumably impacted the [REDACTED] bit, although I cannot independently verify this without Google producing the source code and Google employees with adequate knowledge concerning the engineering and implementation of the [REDACTED] bit (which Google has not done).

¹ “The [REDACTED] field [REDACTED]
[REDACTED] (Benkő Dec. 21, 2022 Decl. ¶ 5).

17. It is also possible that the [REDACTED] bit still functioned well into 2020. On July 21, 2020, Google publicly announced: “As of July 2020, Chrome is gradually rolling out a previously announced fix to address a loophole that could be used by websites to detect Chrome Incognito Mode sessions. The change (Chromium issue #1017120) was first announced in January and will apply to users with Chrome 81+. (Another change announced in January, Chromium issue #990592, rolled out with Chrome 80 in February.)”² This announcement implies that [REDACTED] remained operational until at least Google addressed this “loophole.” Additionally, it appears this “fix” would only impact the functionality of [REDACTED] for Chrome, but not for other browsers. Therefore, [REDACTED] presumably remained operational in Safari, Firefox, Edge, and Edge Legacy as of at least July 2020, if not longer.

18. According to Ms. Benkő, the [REDACTED] “heuristic is by now broken and ineffective for Safari, Chrome, Edge, and Edge Legacy” (Benkő Dec. 21, 2022 Decl. ¶ 6). Benkő did not elaborate on what she meant by “broken” and “ineffective,” nor provide any explanation for how she came to these conclusions. Furthermore, neither Ms. Benkő nor Google have provided an exact date for when the signal became “broken and ineffective.” Since Google did not seek to deprecate the [REDACTED] bit nor its underlying algorithms until late last year (notably after this Court’s class certification decision in December 2022), it is possible that the bit was useful for Google even after the various changes in the underlying API signal.

3. Google’s Refusal to Investigate Additional Bits

19. I understand that the parties have a dispute about whether the Court’s May 20, 2022, sanctions order (Dkt. 588 (the “First Sanctions Order”)) required Google to conduct a full

² Brad Palser, *Protecting Private Browsing in Chrome*, Google News Initiative (July 21, 2020), <https://blog.google/outreach-initiatives/google-news-initiative/protecting-private-browsing-chrome/> (last accessed June 12, 2023).

investigation into logs that contain a private browsing detection bit (Dkt. 898 at 9 (the “Second Sanctions Order”)). Google’s employee charged with completing that investigation, Martin Sramek, admitted that he initially understood the Court’s First Sanctions Order to require a complete investigation into private browsing detection bits and their corresponding logs (Sramek August 18, 2022 Decl. ¶ 7). But Google refused to conduct that investigation and instead limited its investigation to logs that contain the [REDACTED] previously disclosed bits. Google then, through an unexplained and unverified process, identified the [REDACTED] bit through its work on the related *Calhoun v. Google LLC* case (Case No. 4:20-cv-05146) (N.D. Cal.) (Dec. 20, 2022 Ltr. from Google’s Counsel).

20. Based on this series of events, there is no way to definitively know whether there are still-undisclosed private browsing detection bits. To date, Google has yet to provide Plaintiffs with a definitive answer.

21. I also understand that, as a further sanction for Google’s discovery misconduct, the Court’s Second Sanctions Order modified the previously issued jury instruction. The new modified instruction reads:

If in the course of proceedings before the trial judge it is determined that Google’s discovery misconduct is relevant to an issue before the jury, the Court finds the following jury instructions appropriate: (1) “Google failed to disclose to Plaintiffs the names of key Google employees responsible for developing and implementing Google’s Incognito-detection bits”; and (2) “Despite multiple Court orders requiring Google to disclose the information, Google failed to timely disclose (a) at least 70 relevant data sources reflecting the use of three Incognito-detection bits; and (b) at least one additional Incognito-detection bit and any data sources in which it was used. The jury may infer from Google’s failure to disclose these data sources that they are not helpful to Google.”

Dkt. 898 at 12-13. Had Google timely disclosed the [REDACTED] bit and revealed the sources in which it was used, I would have requested data from those logs to conduct a thorough analysis

of that data. My work might have led to additional algorithms and/or bits used by Google to detect private browsing data.

4. The [REDACTED] Bit Supports My Prior Opinions

22. Google's development and use of the [REDACTED] private browsing detection bit further substantiates the following opinions that I have already offered: Opening Report Opinions 1, 2, 4, 5, 6, 7, 8, 17, 18, 19, 20, 22, 24, 25, 26, 27, 29, and 31, and Rebuttal and Supplemental Report Opinions: 1, 3, 5, and 6. These opinions address, among other topics, Google's interception, storage, and use of private browsing data, Google's ability to identify private browsing traffic and class members, and Google's ability to delete the private browsing data it has already collected.

23. The revelation of yet another detection bit is further proof that Google intercepts, stores, and uses private browsing data, and that Google tags this data within its logs as "private." (*e.g.*, Hochman Opening Rep. Opinions 1, 2, 5, and 7). These practices were not disclosed; to the contrary, Google was sanctioned for concealing its use of private browsing detection bits.

24. Google's development and use of the [REDACTED] bit (and private browsing detection bits) contradict public representations that Google and its counsel have made, including:

- "We want you to be able to access the web privately, with the assurance that your choice to do so is private as well" (*See supra* Palser article n.2.).
- "Chrome doesn't tell websites, including Google, when you're browsing privately in Incognito mode" (*How Chrome Incognito Keeps Your Browsing Private*, Google Help Center³).
- "We don't track people in private browsing mode" (Apr. 29, 2021 Hearing Tr. at 25:20-26:13) (statement by Google's counsel)

³ <https://support.google.com/chrome/answer/9845881?hl=en> (last accessed June 12, 2023).

25. Similarly, in the Google blog post I reference above at footnote 2, Google criticized non-Google websites for seeking to detect Incognito browsing; yet Google, through [REDACTED] was using the same exact “loophole” to detect not only Chrome Incognito traffic, but other private browsing mode traffic as well. Plaintiffs even asked a witness in this case about this “loophole”, and he responded that when Google employees discussed Incognito detection, that “always referred to the site you are visiting in Incognito mode, detecting that you are in fact, in Incognito mode” (Schuh Tr. 152:4-23). That deposition occurred in January 2022, before Google disclosed any of the [REDACTED] currently known Incognito detection bits.

26. The Google blog post I reference at footnote 2 is significant for another reason. That blog post supports my opinion that Google intercepts the content of users’ private browsing communications with non-Google websites (Hochman Opening Rep. Opinion 2, § VIII.A). The blog post refers to “articles” on non-Google websites as “content” and criticizes other websites for “intercept[ing]” Incognito mode sessions. Yet, as noted above, Google was simultaneously “intercept[ing]” private browsing communications, logging exactly what users were viewing online (i.e., the “content” of non-Google websites) and tagging that data as “private.”

27. Google’s belated revelation of a private browsing detection bit for non-Chrome browsers is particularly significant because Google criticized me for opining that Google can identify private browsing traffic for Class 2. During my deposition, Google’s lawyer asked me to clarify that “you’re not opining that Google distinguishes between non-Chrome private browsing data and non-Chrome browsing data, correct” (Hochman Tr. 408:21–24). I acknowledged that “I don’t think that I’ve found any incognito detection that relates to non-Chrome browsing” (Hochman Tr. 409:3–9). But I also noted that “[m]aybe there is something that just hasn’t been revealed to us yet.” When Google’s lawyer dismissed my response as “speculation,” I explained that “[i]t’s not

speculation for me to think that you may have withheld something from me when it's already proven that you did withhold stuff from me that was serious. And so it's not speculation. It's an inference." (Hochman Tr. 407:2–408:6).

28. Google's subsequent disclosure of the [REDACTED] bit proves my inference was correct. Google has developed at least one bit aimed at identifying non-Chrome private browsing traffic.

29. Google's behavior with the [REDACTED] bit qualifies as a "side-channel attack."⁴ A side-channel attack is "[a]n attack enabled by leakage of information from a physical cryptosystem." With [REDACTED], Google is exploiting information that leaks from users' browsers for the purpose of identifying that traffic as "private," and Google is using that information for Google's own benefit.

30. Assuming Google preserved the [REDACTED] bit in its logs, or even just the underlying signals used to calculate this bit, Google could use the bit to identify class members, including for Class 2 (non-Chrome private browsing) (*see* Hochman Opening Report § VIII.H). Unlike with the previously identified bits, I never received any data reflecting Google's use of this new bit, so I was not able to conduct a thorough data analysis like I did for the prior bits. But based on the information available to me, I have no reason to doubt that [REDACTED] is reliable,

⁴ *Side-Channel Attack*, Computer Security Resource Center, https://csrc.nist.gov/glossary/term/side_channel_attack (last accessed June 15, 2023). Side channel attacks were originally specific to cryptosystems, but the term has come to be used generally for a computation that utilized unintentionally leaked data from computer software or systems. See for example, *Why side channel analysis attacks are increasing and how to stop them*, Ericsson.com, <https://www.ericsson.com/en/blog/2023/4/side-channel-analysis> (last accessed June 18, 2023), "Side-channel analysis (SCA) is an umbrella term for several different methods of exploiting unintentional information leakage from a process (such as a computer program or application) in a device," and *SMS delivery reports can be used to infer recipient's location*, Bleepingcomputer.com, <https://www.bleepingcomputer.com/news/security/sms-delivery-reports-can-be-used-to-infer-recipients-location/> (last accessed June 18, 2023).

particularly where Google used the bit for years—including perhaps after Plaintiffs filed this case in June 2020. Moreover, my data analysis for the other bits indicate that they detect Incognito traffic extremely accurately (Hochman Rebuttal and Supplemental Report ¶ 28 (99.89% accuracy for `is_chrome_incognito` and `maybe_chrome_incognito` on event-by-event basis)). [REDACTED] is another method for Google to identify private browsing traffic, and, as I have already explained, private browsing data is identifying. (*E.g.*, Hochman Opening Rep. Opinion 22).

31. In addition, if Google preserved the bit or the underlying signal for the bit, it could be used to isolate and delete private browsing data that Google has already collected and is currently storing (Hochman Opening Rep. Opinion 31). This information can be used by the Court to fashion injunctive relief for the Classes, should the Court choose to do so (Hochman Opening Rep. §§ VIII.K, L).

32. The revelation of the [REDACTED] bit also undermines opinions offered by Google’s experts. For example, as I explained in my June 7, 2022, Rebuttal and Supplemental report, Professor Zervas incorrectly opined that private browsing “work[s] as described in public documentation” (Hochman Rebuttal and Supplemental Opinion 6). But as noted above, Google’s private browsing detection practices, including with [REDACTED] contradict Google’s representations to users.

33. Relatedly, Google’s technical expert, Dr. Psounis, cited a W3C guideline which provides that “the use of private browsing mode should not be detectable by websites” (Psounis June 7, 2022 Rebuttal Rep. ¶¶ 70–72). Yet, Google sends itself signals (including the X-Client-Data Header and the [REDACTED] API) and uses these signals to actively detect private browsing data and tag that data as “private,” in violation of the W3C guideline on which its own expert

relied. Dr. Psounis either ignored these Google practices for purposes of his report, or Google withheld this information from him as well.

34. Finally, Google’s concealment of its Incognito detection practices (and its concealment of the [REDACTED] bit in particular) leads me to question what other information Google has from discovery. It is remarkable that, in a case about Google’s practices concerning Incognito, Google during discovery produced:

- [REDACTED] concerning the is_chrome_incognito bit (First Sanctions Order ¶ 124)
- [REDACTED] concerning the is_chrome_non_incognito bit (*id.* ¶ 125)
- [REDACTED] with the term “maybe_chrome_incognito” (database search).

In the same vein, Google produced only [REDACTED] emails sent by Sundar Pichai that contain the word “incognito” (database search). That is surprising given Mr. Pichai’s prior role as the head of Chrome (including while Chrome was released in 2008) and his significant involvement in making decisions about Incognito (*see, e.g.*, Hochman Opening Rep. ¶ 325).

B. [REDACTED] Additional Google Logs with Incognito Detection Bits

1. Google Discloses the Logs, but Does Not Conduct a Full Investigation

35. When I prepared my prior two reports in this case, I was aware of [REDACTED] logs with Incognito detection bits: [REDACTED] for maybe_chrome_incognito, and [REDACTED] for is_chrome_incognito and is_chrome_non_incognito (Hochman Opening Report ¶¶ 144–51). Google did not disclose those [REDACTED] logs until right around when (and after) discovery concluded, and Google was sanctioned in May 2022 for concealing them. After I served my rebuttal and supplemental report on June 7, 2022, Google disclosed an additional [REDACTED] logs that contain Incognito detection bits.

36. Google revealed [REDACTED] of these new logs on June 14, 2022 (June 14, 2022, Sramek Decl.)—following the First Sanctions Order. Google revealed [REDACTED] on November 30, 2022. These [REDACTED] additional logs each contain one of two previously known Incognito detection bits

(is_chrome_non_incognito and maybe_chrome_incognito). In March 2023, Google was sanctioned (a second time) for belatedly disclosing these logs (Dkt. 898).

37. These logs prove that Google’s use of private browsing detection bits, and its storage and use of private browsing data, is more expansive than Google previously disclosed. Google uncovered these additional logs by searching for the three previously known Incognito detection bits in a [REDACTED] table [REDACTED] [REDACTED] (Matthew Harren Nov. 29, 2022 Decl. ¶ 8). Google also restricted its search to bits that relied on the X-Client Data header, which means that Google’s efforts would not reveal bits that rely on other signals, including [REDACTED] (Sramek November 29, 2022 Decl. ¶ 5). Google has never conducted a comprehensive investigation across all logs and data sources (Matthew Harren Nov. 29, 2022 Decl. ¶ 8). As noted above, Google initially interpreted the Court’s First Sanctions Order to require Google to conduct a comprehensive search for private browsing detection bits and corresponding logs, but Google later represented that such a search would have entailed [REDACTED]” and Google has refused to conduct that search (Sramek Aug. 18, 2022 Decl. ¶ 7).

38. I am skeptical of this assertion that it would take “[REDACTED].” Google represents on its website that “Google’s mission is to organize the world’s information and make it universally accessible and useful.”⁵ That cannot be reconciled with Google’s suggestion that it would take [REDACTED] to investigate an internal Google practice surrounding data. And if it were true that it would take [REDACTED] to get to the bottom of it, then I would be

⁵ *Our Approach to Search*, Google, <https://www.google.com/search/howsearchworks/our-approach/> (last accessed June 15, 2023).

concerned because that means that Google does not actually know what Google itself is doing with private browsing data.

39. Google’s representation concedes that Google could have conducted a comprehensive investigation at any time during the discovery period—which lasted for almost two years—leaving Google plenty of time (even under Google’s asserted timeframe). Google could have gone about conducting such an investigation in a variety of ways: For example,

- Google could have identified logs that contain [REDACTED].
- Google could have investigated downstream logs that contain data from the now- [REDACTED] disclosed logs with Incognito detection bits. These downstream logs will likely contain private browsing detection bits as well. As Eugene Lee’s Supplemental Declaration reveals, Google keeps “schematic illustrations of processes that populate certain logs” in “Conflux Workgraphs” (Lee Dec. 19, 2022 Decl. ¶ 3). These Conflux Workgraphs show a detailed relationship between source logs and downstream logs (Lee Dec. 19, 2022 Decl., Exhibit A).
- Google could have investigated other logs that share the same proto structure as the logs containing private browsing detection bits.
- Google could have expanded its search of the [REDACTED] table beyond the [REDACTED] previously known Incognito detection bits. For example, Google could have searched for the word “Incognito”.
- Google could have searched for private browsing bits in its existing Dashboard and databases. In a document Google belatedly produced on November 30, 2022, Google revealed the existence of an “[REDACTED]” that contains [REDACTED] (GOOG-BRWN-00858548 at -553). Google could have used this Dashboard/database to locate any additional fields that may contain the word “Incognito”, and thus uncover additional bits, including any no longer in operation.
- Google could have conducted a diligent and efficient source code search. On February 9, 2023, Steven Ellis submitted a declaration stating that “A search for the string ‘incognito’ across Google source code base yields more than [REDACTED] files” (Ellis Feb. 9, 2023 Decl. ¶ 5). However, Mr. Ellis did not explain whether this search was done across both client-side source code, server-side source code, or both. He could have limited his search to server-side source code (thereby eliminating any reference to Incognito on the browser). Furthermore, he could have limited his search to only source code that impacts the writing of bits into logs from website traffic (as opposed to from non-browser apps and any code that does not impact log writing). Those steps may have significantly reduced the number

of files containing the word “Incognito.” The search Mr. Ellis oversaw was essentially one premised on the idea, “Let’s be as stupid as possible in our search strategy so that we can say this investigation would be impractical.”

40. Moreover, the [REDACTED] logs revealed additional log sources that may contain private browsing data. For example, [REDACTED] of the “[REDACTED] Logs contain data from previously undisclosed logs, including [REDACTED] [REDACTED] [REDACTED] [REDACTED] (Lee Nov. 30, 2022 Decl. ¶¶ 4–8). The [REDACTED] log is [REDACTED] with a previously undisclosed [REDACTED] log to produce undisclosed downstream [REDACTED] log(s) (*Id.* ¶ 11).

41. Had these logs been disclosed earlier, I could have explored their content through the Special Master process to locate additional sources of private browsing data. Because of Google’s untimely disclosure of these [REDACTED] logs, and Google’s refusal to conduct a comprehensive investigation, we do not know the full extent of Google’s storage and use of private browsing data.

2. The [REDACTED] New Logs Support My Prior Opinions

42. Google’s disclosure of these [REDACTED] additional logs with Incognito detection bits further substantiates the following opinions, which I have already offered: Opening Report Opinions 1, 2, 4, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 22, 23, 24, 25, 29, 30, 31; and Rebuttal and Supplemental Opinions 1, 2, 3, 5, and 6. These opinions focus on Google’s interception, storage, and use of private browsing data, as well as Google’s ability to delete the data it has already collected and Google’s ability to destroy algorithms developed through that data.

43. The newly disclosed [REDACTED] logs support my opinions about how private browsing data is identifying. (Hochman Opening Rep. Opinions 18–19, 22; Hochman Rebuttal and Supplemental Rep. Opinions 1, 3, 5). In fact, these logs reveal new information about Google’s data storage architecture, including that Google stores private browsing data in the same log as regular

browsing data. One of the [REDACTED] Logs, the [REDACTED] log, “contains [REDACTED] (Lee Nov. 30, 2022, Decl. ¶ 10). This [REDACTED] log is then further [REDACTED] with the [REDACTED] log to produce [REDACTED] that may also contain Incognito detection bits (*Id.* ¶ 11). While Google itself calls the [REDACTED] log a [REDACTED] Log”, Google argues that “authenticated and unauthenticated records in that file are never joined” (Dkt. 857-03 at 4, Google’s Reply In Response to the Order to Show Cause). This raises the question of why Google calls the log a [REDACTED] but claims there is no [REDACTED]

44. This log further undermines any claim that Google employs best-in-class safeguards to prevent data joining. Based on the evidence available to me as I wrote my opening report, I understood Google’s data storage architecture to store “intercepted data in different logs depending on the signed-in vs. signed-out mode” (Hochman Report ¶ 160). The [REDACTED] [REDACTED] log reveals that Google does not always store signed-in and signed-out data in separate logs; rather, private browsing and regular browsing data, regardless of whether the user is signed-in or signed-out, can all be intermixed within a single log. Put simply, signed-out private browsing data is stored alongside regular browsing data in the same exact log. And there may be more logs like this one; as noted above, Google refused to conduct a comprehensive investigation into these practices, and Google has never stated that no other similar logs exist.

45. The structure of this [REDACTED] also reinforces my opinions about how private browsing data is identifying. The intermixed data are session ordered or sorted (Lee Nov. 30, 2022 Decl. ¶ 10). Consequently, time ordered sequences of events from a user’s signed-out private browsing and signed-in browsing (with the same IP address and user agent, as well as with many of the other parameters I discussed in my opening and rebuttal reports) may appear in sequential order, linking

the signed-out private browsing data with the user's GAIA ID. Private browsing data is even more identifying than I initially understood.

46. Google's practice of storing private browsing data in the same log as regular browsing data also contradicts Google's public representations. For example, prior to the sanctions proceedings in this case, Google represented to the Court that "logs are internally segregated by whether you're logged into a Google account or aren't" (April 29, 2021 Hearing Tr. at 16:19–20). That statement has been proven inaccurate as a technical matter because there is at least [REDACTED] log that contains both signed-out "unauthenticated" data (including private browsing data) and signed-in "authenticated" data. Similarly, Google's testifying expert Dr. Psounis opined that Google "has taken steps to segregate signed-in from signed-out data" (Psounis Rep. ¶ 202). The data is not "segregated." It is stored in the same exact log. Dr. Psounis either overlooked this error in his report, or Google withheld the information from him (as it did from me).

47. The newly disclosed [REDACTED] logs also support my opinions about how Google uses private browsing data to enrich itself. (Hochman Opening Rep. Opinions 11, 12, 13, 14, 17). Indeed, these logs reveal new uses of private browsing data. For example, the [REDACTED] Logs revealed Google's use of private browsing data from third-party exchanges for "modeling and analysis of the functionality of AdWords or DV360 ads served by non-Google exchanges" and Google's use of the data to "evaluate Google's bidding strategy" (Erik Maki Nov. 30, 2022, Decl. ¶ 7). The [REDACTED] Logs reveal Google's use of private browsing data to develop new products by evaluating "how certain ad serving features would behave if the [REDACTED] framework were in place" (Vineet Kahlon Nov. 30, 2022, Decl. ¶ 5). The [REDACTED] Logs reveal Google's use of private browsing data to run hypothetical ad auctions, including [REDACTED] [REDACTED] (Xianzhi Liu Nov. 29, 2022, Decl. ¶ 3).

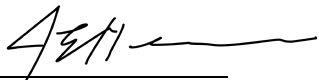
48. These newly disclosed uses of private browsing data further undermine any claim that Google has publicly disclosed the full extent of its collection, storage, and use of private browsing data, particularly where Google was twice sanctioned for concealing the full scope of these practices, and where Google still refuses to provide complete discovery, such as by conducting a fulsome investigation.

49. Finally, these ■ logs, and the uses of the data which they reveal, provide additional pathways for the Court to fashion injunctive relief, should the Court choose to do so (Hochman Opening Rep. §§ VIII.K, L). For example, Google could be ordered to cease using private browsing data for the purposes listed above, and Google could be ordered to delete any private browsing data stored in these ■ logs. Google could also be ordered to conduct a fulsome investigation into its collection, storage, and use of private browsing data—an investigation that it has conceded is possible. That investigation may in turn yield additional bits, logs, and/or uses, including algorithms and models that could be ordered destroyed.

* * *

50. My investigation is ongoing. I reserve the right to update or supplement this report in reliance upon whatever further information becomes available.

Respectfully submitted by,

/s/ 

JE Hochman & Associates LLC

Date: June 20, 2023

EXHIBIT A

JONATHAN E. HOCHMAN

jonathan@hochmanconsultants.com

Tel +1-203-699-2628

CURRENT POSITIONS

- 2004 – Present HOCHMAN CONSULTANTS – Partner
Founded Internet and search marketing agency as outgrowth of prior position. Provides consulting and software development services to clients, including technology companies, publishers, ecommerce providers and web development firms.
- 2018 – Present UNS PROJECT – Co-Founder
Invented and developed Internet infrastructure service for user authentication, linking of de-identified records, and detection of fake accounts.

PAST POSITIONS

- 2010 – 2018 CODEGUARD, INC. – Co-Founder – Acquired by Sectigo and Francisco Partners
Invented web site security service, built working prototype, and raised initial capital.
- 2008 – 2019 SEMNE (SEARCH ENGINE MARKETING NEW ENGLAND) – Chair and
Founding member of search marketing association in New England.
- 1999 – 2004 BARCODING INC. – Director
Systems integrator provides software, bar code technology, RFID technology, and wireless networks to commercial, manufacturing, warehousing, and government sectors. Named to the Inc. 500 (Nov 2004). Recognized by Forbes Magazine as one of ten privately held companies to watch (Feb 2004). Ranked third on the Maryland Fast 50. Raised 50% of initial funding to grow the business from two to sixty employees.
- 1999 – 2003 UNITED ALLOYS CORPORATION – General Manager
Imported specialty metals and chemicals for sale in North America on behalf of Russian producers.
- 1996 – 1999 INDUSTRIAL METALS & CHEMICALS CORPORATION – General Manager
Sales and marketing of specialty metals and chemicals representing Russian producer worldwide.
- 1990 – 1996 NORTH ATLANTIC RESOURCES, INC. – President
Consulting firm assisted Russian companies with foreign trade in Europe, North America, Middle East, and Asia. Products sold included mainframe computers, software, office equipment, consumer electronics, consumer packaged goods, and construction materials.

EDUCATION

- 2022 – Present YALE UNIVERSITY
PhD student in the Yale Applied Cryptography Laboratory (starting August 22, 2022).
- 1990 – 1991 COLUMBIA LAW SCHOOL
Completed first year of law school, then departed to spend time managing own venture.
- 1986 – 1990 YALE UNIVERSITY
Co-terminating BSc. and MSc. degrees in Computer Science awarded *summa cum laude*, distinction in the major, Tau Beta Pi (The Engineering Honor Society), Barge Mathematics Prize, Henry Edwards Ellsworth Memorial prize for significant research.

CERTIFICATES

1. CITI Program, Biomedical Research – Basic 50611315, issued Jan 11, 2023, expiry Jan 11, 2026
2. Google Ads Display Certification – Credential ID 108990524, issued March 21, 2022, expiry March 21, 2023
3. Google Ads Search Certification – Credential ID 109000107, issued March 21, 2022, expiry March 21, 2023

ACADEMIC PAPERS

1. Fischer M.J., Hochman J.E., Boffa D. (2021) Privacy-Preserving Data Sharing for Medical Research. Stabilization, Safety, and Security of Distributed Systems. SSS 2021. Lecture Notes in Computer Science, vol 13046. Springer, Cham. <https://doi.org/10.1007/978-3-030-91081-5>
2. How to Create a Failure Tolerant Distributed System, Jonathan E. Hochman, Yale University Department of Computer Science Tech Report 799, April 1990

PUBLISHED ARTICLES

1. New Wave of Referrer Spam Wrecking Google Analytics Data, Marketing Land, December 8, 2016
2. What is Search Engine Optimization Manipulation, National Law Review, May 18, 2016
3. A Proposal for Ethical Ad Blocking, Marketing Land, October 5, 2015
4. Web Overload: Why Digital Advertising Needs to Hit the Reset Button, Marketing Land, September 25, 2015
5. Pay-to-Unpublish Sites Practice 'Digital Blackmail', Internet Evolution, November 6, 2013
6. Why Google Should Crack Down Harder On The Mugshot Extortion Racket, Search Engine Land, Feb. 6, 2013
7. How to Avoid Enterprise Password Danger, Internet Evolution, June 27, 2012
8. Tech Group's Open Letter to Its Congressman, Internet Evolution, January 19, 2012
9. SEO Service Spammers: Combating Disinformation, Search Marketing Standard, Winter 2011/2012
10. Deconstructing Microsoft AdCenter's Missed Opportunities, Search Engine Land, February 17, 2011
11. What Every Search Marketer Needs to Know About Web Security, Search Engine Land, December 30, 2010
12. 5 SEO Tips You Can Usually Ignore, Search Marketing Standard, Summer 2010
13. How To Avoid Getting Your Search Rankings Trashed by Malware, Search Engine Land, Sept. 4, 2009
14. Google Turns Blind Eye to Scam Ads, Internet Evolution, Aug. 21, 2009
15. Nasty Malware Attack Targets Web Developers, Internet Evolution, Aug. 19, 2009
16. An Open Letter to Online Ad Networks, SEBOOK, July 28, 2009
17. Simple Security Steps to Stop Server Spam, Internet Evolution, July 23, 2009
18. How to Protect Your Web Marketing Assets, Internet Evolution, March 4, 2009
19. An Update on JavaScript Menus And SEO, Search Engine Land, January 9, 2009
20. Is Wikipedia Transparent Enough?, Search Marketing Standard, Winter 2008/2009
21. Google SearchWiki - Opportunity or Headache, Search Marketing Standard, Spring 2009
22. Microsoft Announces adCenter Desktop Beta during SMX Advanced Keynote, Search Engine Land, June 2, 2008
23. Twelve Simple Ways to Write Search-Friendly HTML Code, Search Engine Land, May 30, 2008
24. Legitimate, Useful Subversion for Search Engine Marketers, Search Engine Land, April 8, 2008
25. Using Wikipedia to Reveal Web Traffic Data, Search Engine Land, March 12, 2008
26. Virtual Blight & The Ten Commandments for Online Marketers, Search Engine Land, February 18, 2008
27. URL Rewriting & Custom Error Pages in ASP.NET 2.0, Search Engine Land, September 21, 2007
28. Microsoft adCenter Offers Appealing Upgrade, Search Engine Land, September 10, 2007
29. Tracking Hot Topics on Wikipedia, Search Engine Land, September 10, 2007
30. Search Marketing & Web Page Download Speed, Search Engine Land, September 5, 2007
31. How to Get More Pages into Google's Index, Search Engine Watch, August 1, 2007

SELF-PUBLISHED ARTICLES

1. The Cost of Pay Per Click Advertising— PPC Trends and Analysis
2. 302 Redirect vs. 301 Redirect: Which is Better?
3. How to Get Google Sitelinks
4. How to Standardize Multiple Domains for SEO Using 301 Redirects
5. How to Write Meta Descriptions (Code Sample Included)
6. The Cost of Banner Advertising – Trends and Analysis

7. Basic SEO Tips
8. The Benefits of Clean URLs
9. Best Content Management Systems and SEO
10. Best Practices for Managing Online Reviews
11. The Cost of SEO Services
12. External Links & SEO
13. Adobe Flash and SEO
14. The Google Sandbox Effect
15. How to Block Part of a Page from Being Indexed by Google or Other Search Engines
16. The Internet Marketing Process
17. The Danger of Deadlines in Web Development
18. Spam Prevention Techniques

SPEAKING

1. Yale Innovation Summit, New Haven, May 2022
2. 23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems, November 2021
3. Yale Innovation Summit, New Haven, May 2019
4. VT Web Marketing Summit, Burlington, VT, November 2017
5. National Expert Witness Conference, Clearwater Beach, FL, May 2017
6. International Printing & Imaging Conference, Henderson, NV, July 2016
7. VT Web Marketing Summit, Burlington, VT, November 2015
8. VT/NH Marketing Group, Woodstock, VT, May 2015
9. VT Web Marketing Summit, Burlington, VT, November 2014
10. VT Web Marketing Summit, Burlington, VT, November 2013
11. VT/NH Marketing Group, Whitefield, NH, June 2013
12. VT Web Marketing Summit, Burlington, VT, November 2012
13. SMX East, New York, October 2012
14. SMX Advanced, Seattle, June 2012
15. SMX West, San Jose, Feb 2012
16. SMX Advanced, London, May 2011
17. SMX Toronto, April 2011
18. SMX West, San Jose, March 2011
19. SMX West, Santa Clara, March 2010
20. IWLA Marketing and Sales Conference, Chicago, July 2009
21. SMX Advanced, Seattle, June 2009
22. Web 2.0 Expo, San Francisco April 2009
23. Web 2.0 Summit, November 2008
24. SMX East, New York, October 2008
25. SMX Advanced, Seattle, June 2008
26. SMX Social Media, Long Beach, April 2008
27. Search Engine Strategies, San Jose, August 2007
28. Search Engine Strategies, New York, April 2007
29. Search Engine Strategies, Chicago 2006
30. IWLA Marketing and Sales Conference, Chicago, July 2006

PATENTS AND PATENT APPLICATIONS

1. Systems and Methods for Secure Data Sharing, Provisional US Patent Application No. 63280955
2. User Authentication System, Patent No. US11570163.
3. Systems and methods for automated retrieval, monitoring, and storage of online content, Patent No. US9069885B1
4. Wireless collection of battery performance metrics system, method, and computer program product Publication No. US20050027466A1

TRIAL TESTIMONY

1. **Take 5 Media, et al.** v. Advantage Sales & Marketing, et al., AAA No. 01-19-0002-7532.
2. **Client 5** v Party 5, American Arbitration Association, Case 01-20-15-5410.
3. Social Tokens v. **VDOPIA**, Tel Aviv-Jaffa Magistrate's Court (2021).
4. Boppers v. **Rosenay**, HHD-CV19-60104115-S, Connecticut Superior Court, Judicial District of Hartford.
5. **Loytr** v. TinyCo, CGC-16-551519, Superior Court of California, County of San Francisco.
6. **Borg** v. Cloutier, FST-CV-16-6028856-S, Connecticut Superior Court, Judicial District of Stamford.
7. **Client 2** v Party 2, binding private arbitration, Glendale, CA.
8. Party 3 v **Client 3**, binding private arbitration, Austin, TX.
9. The H&M Law Firm v. **Venning**, BC577241, Superior Court of California, County of Los Angeles.
10. General Steel v. **Chumley**, 13-00769, US District Court for the District of Colorado.
11. PODS v. **U-Haul**, 8:12-01479, US District Court for the Middle District of Florida.
12. **Client 1** v Party 1, binding private arbitration, Miami, FL.

DEPOSITION TESTIMONY

1. Edible v **800-FLOWERS**, 1:20-cv-2405, , US District Court for the Northern District of Georgia.
2. **Delta** v Marriott, 1:20-CV-01125, US District Court for the Northern District of Georgia.
3. Tireboots by Universal Canvas v. **Tiresocks**, 1:20-cv-07404, US District Court for the Northern District of Illinois.
4. **Client 6** v Party 6, binding private arbitration, March 2023.
5. Damian v. **Courtright**, 1:21-cv-01694, US District Court for the Northern District of Illinois.
6. **Iraida Hernandez** v Ashish Pal, M.D., 2020-CA-10122-O, Circuit Court, Orange County, Florida
7. **Premier Automotive** v DealerCMO, 19CV344119, Superior Court of California, County of Santa Clara.
8. San Juan Products v **River Pools & Spas**, 8:21-cv-02469, US District Court for the Middle District of Florida.
9. What a Smoke v **Duracell**, 2:19 cv 16657, US District Court for District of New Jersey.
10. **Evox** v AOL, 20-cv-02907, US District Court for the Central District of California. (Supplemental Report)
11. **Brown** v Google, 20-cv-03664, US District Court for the Northern District of California.
12. **Black** v CNN, 5016CA001517, Circuit Court of the Fifteenth Judicial Circuit, Palm Beach County, Florida.
13. Legno Bastone v **Provenza Floors**, 20-CA01486, Circuit Court, 20th Judicial Circuit, Collier County, Florida.
14. **Drips** v Teledrip, 5:19-CV-02789, US District Court for the Northern District of Ohio, Eastern Division.
15. **Lane** v Elyassnia, et al., CGC-20-586918, Superior Court of California, County of San Francisco.
16. **Take 5 Media** v. Advantage Sales & Marketing, et al., AAA No. 01-19-0002-7532.
17. Honey Baked Ham Inc. v. **Honey Baked Ham Company LLC**, 8:19-cv-01538, US District Court, Central District of California, Southern Division.
18. **National Rifle Association of America** v. Ackerman McQueen Inc et al, 3:19-cv-02074, US District Court, Northern District of Texas, Dallas Division.
19. **Evox** v AOL, 20-cv-02907, US District Court for the Central District of California.
20. Party 4 v **Client 4**, binding private arbitration.
21. **Zillow** v IBM, IPR2020-01656, USPTO, Patent Trial and Appeal Board.
22. **Zillow** v IBM, IPR2020-01655, USPTO, Patent Trial and Appeal Board.
23. **FurnitureDealer.Net** v Amazon.com and COA Inc, 18-cv-00232, US District Court, Minnesota.
24. **H. Roske** v Christian Burghart, 657328/2017, Supreme Court of New York, New York County.
25. RingCentral v **Nextiva**, 19-cv-02626, US District Court for the Northern District of California.
26. **Davis and Azar** v Yelp, 18-cv-00400, US District Court for the Northern District of California.
27. **Jayda Cheaves** v Walgreens, 19-cv-02970, US District Court for the Northern District of Georgia.
28. Penn Engineering v **Peninsula Components**, 19-cv-00513, US District Court, Eastern District of Pennsylvania.
29. American Airlines v **Delta Air Lines**, 19-cv-01053, US District Court for the Northern District of Texas.
30. Troubleshooter Network v **HomeAdvisor**, 18-cv-02362, US District Court for the District of Colorado.
31. Hotel Airport v **Best Western International**, 2:19-cv-01393, US District Court for the District of Arizona.
32. **Dreamstime** v Google, 3:18-cv-01910, US District Court for the Northern District of California.
33. In re Snap Securities Litigation (for **lead plaintiffs and the class**), 2:17-cv-03679, US District Court, Central District of California.
34. Gree v **Supercell**, IPR2019-00086, USPTO, Patent Trial and Appeal Board.

35. Gree v **Supercell**, IPR2019-00083, USPTO, Patent Trial and Appeal Board.
36. **Ascente** v Digital River, 18-cv-00138, US District Court for the District of Minnesota.
37. **Williamson** v Google, 3:15-cv-00966, US District Court for the Northern District of California.
38. Tempur-Pedic v **Mattress Firm**, 4:17-cv-1068, US District Court for the Southern District of Texas.
39. **Leadership Studies** v. Blanchard, 15-cv-1831, US District Court for the Southern District of California.
40. **Loytr** v TinyCo, CGC-16-551519, Superior Court of California, County of San Francisco.
41. **Borg** v Cloutier, FST-CV-16-6028856-S, Connecticut Superior Court, Judicial District of Stamford.
42. Linkepic v **Wittstrom and Tannehill**, 12-cv-9058, US District Court for the Northern District of Illinois.
43. Hooked Media Group v **Apple**, 114CV265819, Superior Court of California, County of Santa Clara.
44. Pensler v **Fox Television**, 11 L 009425, Circuit Court of Cook County, IL.
45. **Client 2** v Party 2, binding private arbitration.
46. Telebrands v **Tinnus Enterprises**, PGR2015-00016, USPTO, Patent Trial and Appeal Board.
47. Edible Arrangements v **1-800-Flowers.Com**, 3:14-01744, US District Court for the District of Connecticut.
48. **Concordia Partners** v Marcelle Pick, 2:14-00009, US District Court for the District of Maine.
49. General Steel v **Ethan Daniel Chumley**, 14-01932, US District Court for the District of Colorado.
50. **Client 1** v Party 1, binding private arbitration.
51. Kelly-Brown v **Oprah Winfrey**, 1:11-07875, US District Court for the Southern District of New York.
52. PODS v **U-Haul**, 8:12-01479, US District Court for the Middle District of Florida.

Retaining parties shown in bold.